

УДК 530.145

Д. Є. Котлов, студент гр. ПК-71
КПІ ім. Ігоря Сікорського

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ TRUSTED WIRELESS В РОБОТОТЕХНІЧНИХ СИСТЕМАХ НЕРУЙНІВНОГО КОНТРОЛЮ

Анотація. У роботі розглядаються перспективи впровадження бездротових систем у неруйнівному контролі, існуючі технологічні та інженерні рішення для даної теми та стислий їх опис. Наводиться список сучасних обмежень в області неруйнівного контролю та рішення, які може надати використання бездротових технологій Trusted Wireless.

Ключові слова: неруйнівний контроль, бездротові системи, робототехніка, Trusted Wireless

ВСТУП

В системах неруйнівного контролю поступово відбувається перехід від ручного до автоматизованого керування приладами контролю. Це прибирає деякі обмеження, що були пов'язані з людським фактором, проте залишає відкритим питання обмежень, що накладаються на систему дротовим з'єднанням. З метою розширення можливостей автоматизації контролю з використанням робототехнічних комплексів можуть бути використані бездротові системи керування.

Мета даної роботи – розглянути сучасні інженерні рішення під час створення систем бездротової передачі інформації, їх переваги та недоліки, а також принцип роботи та можливості, які вони надають у сфері роботизації і автоматизації неруйнівного контролю та діагностики.

ОГЛЯД ПОПЕРЕДНІХ РОБІТ

В останні роки проводиться багато досліджень в області локальної передачі даних з пристроїв неруйнівного контролю на портативні пристрої, зокрема через мережу Bluetooth та Wi-Fi. Зокрема, приклади використання бездротових технологій в автоматизованих системах неруйнівного контролю наведені в роботах [1, 2]. Такі системи є складовими більш складних комплексів, що включають в себе багато сенсорів, які зазвичай пов'язані між собою та сервером мережею.

Сучасне виробництво характеризується великою кількістю електромагнітних шумів. Проте такі шуми зазвичай не є завадою для бездротових систем Wi-Fi, які працюють у діапазоні частот 2.4 ГГц, поділеному на 14 каналів (по 22 МГц кожен). Однак, джерелом завад можуть стати інші бездротові системи, які оперують на такій самій частоті. З метою забезпечення сумісності систем, Wi-Fi використовує широкосмугову модуляцію з прямим розширенням спектра (Direct Sequence Spread Spectrum, скорочено DSSS). У випадку такої модуляції відбувається розширення спектру внаслідок заміни 1 біту інформації декількома. Перевагою DSSS модуляції є висока швидкість передачі даних. Проте недоліком є те, що вона внаслідок розширення спектра може повноцінно безперебійно функціонувати лише максимум за 3-х мереж Wi-Fi. Другим недоліком є те, що така система погано суміщається з іншими системами, які будуть розглянуті пізніше, через значну ширину спектру.

Однією з систем, які дають змогу побудови бездротових мереж, є обладнання компанії Phoenix Contact [3]. Такі параметри Wi-Fi, як швидкість та відстань передачі даних сильно варіюються та можуть досягати декількох Гбіт/с на відстань декількох кілометрів (проте це значно ускладнює налаштування системи), при чому відстань обернено пропорційна до швидкості. Також у Wi-Fi є можливість встановлення структури 'mesh' (сітка, рис. 2), за якої відбувається автоматичне підключення до найближчої точки доступу в мережі, але не має можливості контролювати таке підключення. Принцип роботи цієї структури полягає в тому, що підключення пристроїв (S) відбувається не тільки напряму до джерела сигналу (M), а й до повторювачів (R), які дублюють сигнал джерела або іншого повторювача, тим самим розширюючи зону покриття мережі.

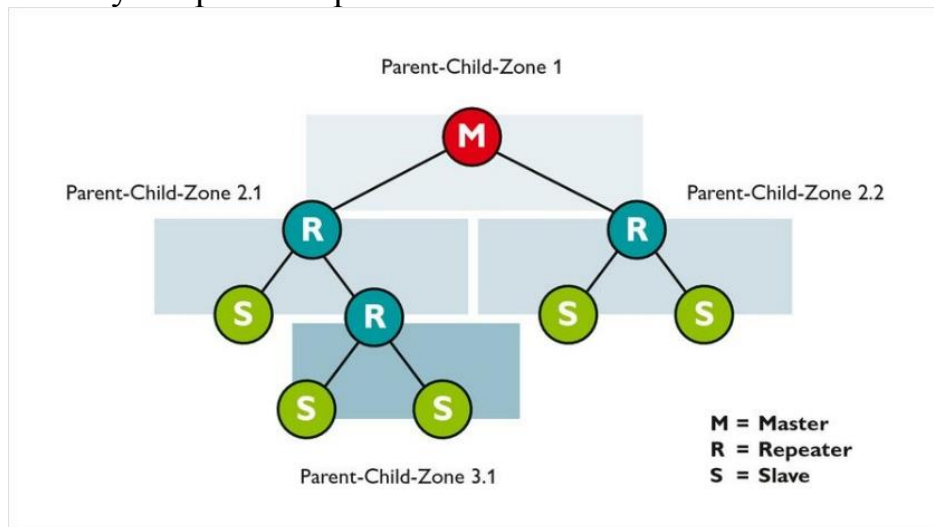


Рис 1. 'Mesh' структура

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На основі огляду попередніх робіт можна зробити висновок, що перевагами бездротових систем перед дротовими є: відсутність необхідності у додатковому просторі для дроту; мінімальна кількість монтажних робіт; мобільність системи; незалежність від конкретної зовнішньої системи керування; можливість зовнішньої обробки інформації на віддаленому сервері; можливість автоматизації через впровадження таких сучасних методик, як нейронні мережі завдяки доступності збору та аналізу статистичних даних [4]. Водночас, недоліками бездротових систем є: відсутність постійного живлення системи; більша вартість обладнання; менша швидкість передачі даних, яка може залежати від середи розповсюдження сигналу.

На даний момент існує багато стандартів технології бездротового зв'язку, які визначаються робочим діапазоном, швидкістю передачі даних, кількістю каналів та площею покриття, проте вони в загальному випадку мають різні області застосування. У промисловості у складі автоматизованих систем неруйнівного контролю перспективно використовувати протокол Trusted Wireless 2.0, який володіє нижчою швидкістю передачі даних у порівнянні з Wi-Fi або Bluetooth, проте мають ряд важливих особливостей.

На відміну від Wi-Fi, Trusted Wireless 2.0 використовує модуляцію з псевдовипадковою перебудовою робочої частоти (Frequency Hopping Spread Spectrum, FHSS), у разі застосування якої завади будуть впливати лише на одну з частот, незалежно від ширини спектру [5]. Даний принцип показано на рис. 2. А враховуючи, що на відміну від 14 каналів Wi-Fi, Trusted Wireless 2.0 має 127 каналів, можна прийти до висновку, що така система є більш завадостійкою у випадку значних рівнів шумів. Це особливо ефективно на промислових ділянках, через те що такі процеси, як зварювання, можуть генерувати шуми з дуже широким спектром.

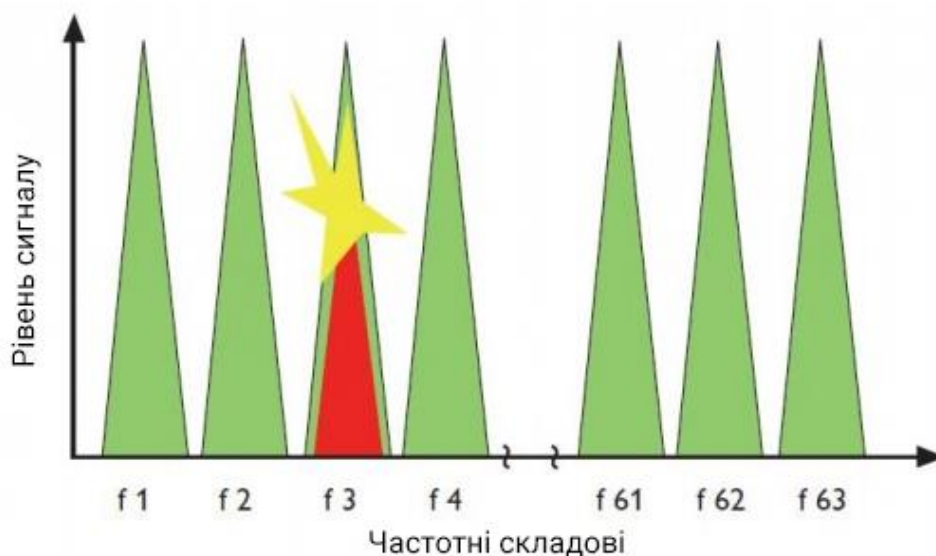


Рис 1. Вплив завад у випадку FHSS

Перевагою Trusted Wireless 2.0 також є те, що вона набагато краще суміщається з іншими мережами завдяки великій кількості каналів, а також дає можливість ігнорувати деякі частоти, що також грає роль під час створення структури 'mesh', яка в такому випадку буде позбавлена недоліку відповідної структури Wi-Fi.

Проте однією з головних переваг Trusted Wireless 2.0 є те, що вона дозволяє передавати дані на дуже далекі відстані (до 5 км за швидкості 16 кбіт/с). Швидкість передачі даних невисока, але у роботизованих системах неруйнівного контролю, які зазвичай оперують лише набором діагностичних значень, швидкість не є критичним параметром [6].

Ще однією особливістю Trusted Wireless 2.0 є відсутність відкритого доступу до протоколу та шифрування даних з ціллю захисту від зовнішніх вторгнень до системи (в тому числі перехвату та зміни даних). Це дуже важливо на промислових елементах, робота яких може повністю зупинитися у разі зовнішнього втручання, яке особливо легко виконати за невеликого об'єму даних, що проходять в мережі.

Таким чином, у сфері автоматизації неруйнівного контролю вигідно використовувати саме завадостійкі, а не обов'язково швидкі системи. А завдяки зручній внутрішній структурі мережі можливе проведення багатьох процедур контролю паралельно з опрацюванням великої кількості даних.

ВИСНОВКИ

Розглянута технологія Trusted Wireless дозволить спростити структуру автоматизованої системи контролю завдяки перенесенню розрахунків та візуалізації даних на зовнішню периферію. Дальність дії технології дозволяє використовувати її для управління робототехнічними комплексами, які можуть використовуватися для проведення неруйнівного контролю на великих за площею виробництвах чи об'єктах.

Крім того, перспективною є повна автоматизація виробництва за рахунок об'єднання в єдину мережу, що відповідає концепції Індустрії 4.0. Обробка даних на сервері дозволить впровадити нові інженерні рішення, наприклад, для підвищення точності результатів за рахунок статистичного або інтелектуального аналізу даних. Проте підвищення складності системи призведе до збільшення об'ємів оброблюваної інформації, тому серед напрямів розвитку можна виокремити підвищення швидкості передачі даних та покращення зв'язку між елементами внутрішньої мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Петрик, В.Ф. Мобильный вихретоковый дефектоскоп с беспроводной системой передачи данных / В.Ф. Петрик, А.Л.Дугин, В.В.Карпинский, А.Л. Кустовский, Ю.Ю. Лисенко // Журнал «Научни Известия НТСМ» : материалы международной конференции «Дни НК 2016», г. Созополь, 2016 г. - Созополь, 2016. - № 1(187) - С. 43 - 45.
- [2] Povshenko, O. Portable Ultrasound Flaw Detector / O. Povshenko, V. Petryk, A. Protasov // Неруйнівний контроль в контексті асоційованого членства України в Європейському Союзі: матеріали 2-гої науково-технічної конференції, Польща, м. Люблін, 15-19 жовтня 2018 року. - Люблін, Польща, 2018.-С. 34-36.
- [3] Shapo V. Teaching and Learning of Industrial Cyber Security Technologies Based on Phoenix Contact Company Wireless Equipment / V. Shapo, M. Levinskyi, V. Volovshchikov. // JOURNAL OF SCIENTIFIC PERSPECTIVES. – 2020. – №4. – С. 99–110.
- [4] Momot A. S. The Use of Backpropagation Artificial Neural Networks in Thermal Tomography / A. S. Momot, R.M. Galagan. // proc. 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC) Kiev, 8-12 October 2018 / IEEE. – 2018. – pp. 1–6.
- [5] Trusted Wireless 2.0 by Phoenix Contact – Режим доступа:
- [6] https://www.phoenixcontact.com/online/portal/ru?ldmy&urile=wcm:path:/ruru/web/main/products/technology_pages/subcategory_pages/Industrial_wireless_trusted_wireless_20/4883facb-f018-41b1-ab09-f30f0313d9d3
- [7] Toward trusted wireless sensor networks / [W. Hu, H. Tan, P. Corke et.al.]. // ACM Transactions on Sensor Networks. – 2010. – №7. – С. 25–35.

Наук. керівник – доктор філософії, ас. Момот А.С.